The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/21/2012

SUBJECT:
Denial of Service Vulnerability in Cisco ASA products

OVERVIEW:
A denial of service vulnerability has been discovered in Cisco Adaptive Security Appliance (ASA) 5500 series appliances and ASA modules for Catalyst 6500 series switches (ASASM). Cisco ASA products provide firewall, intrusion prevention, remote access, and other services. Successful exploitation could result in denial of service conditions or a reload on the affected device.

SYSTEMS AFFECTED:

- Cisco ASA 5500 Series Appliances running software versions prior to 8.4 (4.1), 8.5 (1.11), and 8.6 (1.3)
- Cisco Catalyst 6500 series ASA Service Modules running software versions prior to 8.4 (4.1), 8.5 (1.11), and 8.6 (1.3)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

DESCRIPTION:
Cisco ASA 5500 series appliances and Cisco Catalyst 6500 Series ASA Service Modules (ASASM) are prone to a remote Denial of Service vulnerability due to the improper handling of IPv6 traffic. This issue occurs when the devices are running in transparent mode with IPv6 enabled and have system logging configured to log message ID 110003 (enabled with logging severity level 6 or higher). These settings are not enabled by default. To exploit this vulnerability, an attacker creates a specially crafted IPv6 packet that will generate log message ID 110003 and sends it to the vulnerable device. When the packet is processed, the log message is created resulting in denial of service conditions or a potential reboot of the device.

Information related to log message ID 110003 can be found at hxxp://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.html#wp4769354.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Cisco after appropriate testing. To view a complete list of what software fixes to apply, please see hxxp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaIPv6
- Consider disabled log message ID 110003 by issuing the "no logging message 110003 command". To view the instructions for this workaround please see hxxp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaIPv6

REFERENCES:

Cisco:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaIPv6#@ID
http://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.html#wp4769354

Security Focus:

http://www.securityfocus.com/bid/54106

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3058